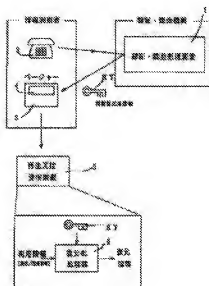


CERTIFYING/CHARGING METHOD FOR INFORMATION USER, METHOD FOR DISTRIBUTING INFORMATION FOR INFORMATION RESTORATION TO INFORMATION USER, RADIO CALLING DEVICE AND REPRODUCING OR RECEIVING DEVICE

Patent number: JP11331150 (A)
 Publication date: 1999-11-30
 Inventor(s): KORI TERUHIKO +
 Applicant(s): SONY CORP +
 Classification:
 - international: G06F21/24; G09C1/00; H04H20/74; H04H20/76; H04H20/21; H04H20/23; H04L9/32; H04Q7/10; H04Q7/20; H04Q7/38; G06F21/00; G09C1/00; H04H1/00; H04L9/32; H04Q7/06; H04Q7/20; H04Q7/38; (IPC1-7): G09C1/00; H04H1/00; H04L9/32; H04Q7/10; H04Q7/20; H04Q7/38
 - european:
 Application number: JP1990130274 19900513
 Priority number(s): JP1990130274 19900513

Abstract of JP 11331150 (A)

PROBLEM TO BE SOLVED: To secure a communication means between a certifying/charging institution and a user through a simple method, in utilizing information. **SOLUTION:** For this certifying/charging method, an information user reports personal information, including identification information for identifying the information user and information required for charging and identification information previously applied for specifying information or the information contents to be defined as a utilization object through a telephone line to the certifying/charging institution. After the substance or client of utilization is specified based on this information, the certifying/charging institution distributes information for information restoration for every information defined as the utilization object to the information user through a radio call to that user. The information user cancels the enciphering applied to the utilization information, through the use of the received information for information restoration.



Data supplied from the **espacenet** database — Worldwide

特開平11-331150

(43)公開日 平成11年(1999)11月30日

(51)Int.Cl. ⁶	識別記号	P I
H 0 4 L 9/32		H 0 4 L 9/00 6 / 3 A
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 B
H 0 4 Q 7/38		H 0 4 I 1 1/02 F
H 0 4 H 1/02		H 0 4 B 7/26 1 0 9 S
H 0 4 Q 7/10		H 0 4 Q 7/02 B
審査請求 未請求 請求項の数14 O L (全 10 頁) 最終頁に続く		

(21)出願番号 特願平10-130274

(22)出願日 平成10年(1998)5月13日

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 都 照彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

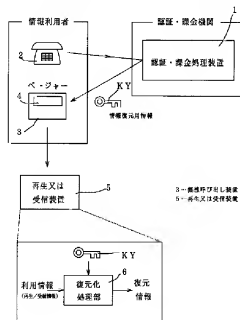
(74)代理人 弁理士 小松 祐治

(54)【発明の名称】 情報利用者についての認証・課金方法、情報利用者への情報復元情報の配布方法及び無線呼び出し装置、並びに再生又は受信装置

(57)【要約】

【課題】 情報の利用にあたって、簡易な方法で認証・課金機関と利用者との間の通信手段を確保する。

【解決手段】 情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報と、利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知する。認証・課金機関はこれによって利用主体及び客体を特定した後、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報を配布する。情報利用者は受信した情報復元用情報を用いて利用情報に施された暗号化を解除する。



【特許請求の範囲】

【請求項1】 情報利用者の加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者の個人情報や利用状況情報を管理するための、情報利用者についての認証・課金方法において、

情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報と、利用対象とされる情報又は当該情報内容を持つために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知することによって、認証・課金機関が利用主体及び客体を特定することと特徴とする情報利用者についての認証・課金方法。

【請求項2】 請求項1に記載した情報利用者についての認証・課金方法において、

情報利用者が、電話回線を通して認証・課金機関にパスワードを送出し、認証・課金機関が当該パスワードを、情報利用者について予め設定されているパスワードと照合することによって当該利用者の確認を行うことを特徴とする情報利用者についての認証・課金方法。

【請求項3】 情報利用者に対してその加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報を配布することを特徴とする情報利用者への情報復元用情報の配布方法。

【請求項4】 請求項3に記載した情報利用者への情報復元用情報の配布方法において、

(イ) 利用対象とされる情報毎に付与される情報復元用情報を、認証・課金機関と情報利用者との間で通用する鍵情報を用いて認証・課金機関が暗号化した後、

(ロ) (イ)で暗号化された情報復元用情報を、認証・課金機関が情報利用者への無線呼び出しによって当該利用者へ通知し、

(ハ) (ロ)で通知された情報復元情報に施された暗号化を、情報利用者が(イ)の鍵情報と同じ鍵情報を用いて解除することを特徴とする情報利用者への情報復元用情報の配布方法。

【請求項5】 請求項3に記載した方法に使用する無線呼び出し装置であって、

利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報及び利用対象とされる情報の情報復元用情報を、認証・課金機関から受信するとともに、これらの情報を文字情報として表示することを特徴とする無線呼び出し装置。

【請求項6】 請求項4に記載した方法に使用する無線呼び出し装置であって、

利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報及び暗号化された情報復元用情報を、認証・課金機関から受信するとともに、これらの情報を文字情報として表示することを特徴とする

無線呼び出し装置。

【請求項7】 請求項3に記載した方法に使用する無線呼び出し装置であって、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項8】 請求項4に記載した方法に使用する無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項9】 請求項5に記載した無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項10】 請求項6に記載した無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項11】 請求項3に記載した方法に使用する再生又は受信装置であって、

利用対象とされる情報の情報復元用情報が入力された場合に、当該情報に基づいて利用対象とされる情報の復元化処理を行うことを特徴とする再生又は受信装置。

【請求項12】 請求項4に記載した方法に使用する再生又は受信装置であって、

暗号化された情報復元用情報が入力された場合に、該情報に施された暗号化を、予め設定されている鍵情報を用いて解除するとともに、当該情報に基づいて利用対象とされる情報の復元化処理を行うことを特徴とする再生又は受信装置。

【請求項13】 請求項11に記載した再生又は受信装置において、

利用対象とされる情報について無線呼び出し装置で受信した情報復元用情報を装置内に取り込むための受信手段を備えていることを特徴とする再生又は受信装置。

【請求項14】 請求項12に記載した再生又は受信装置において、

利用対象とされる情報について無線呼び出し装置で受信した情報復元用情報を装置内に取り込むための受信手段を備えていることを特徴とする再生又は受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報利用者についての認証・課金方法や情報利用者への情報復元用情報（暗号解読鍵等）の配布方法に関するものである。

【0002】

【従来の技術】 デジタル化された音声情報や映像情報

等の再生や受信において、従来の方法では再生装置や受信装置の利用者の認証・課金について専用の情報記録媒体や装置を用いる必要がある。

【0003】例えば、デジタル衛星放送受信機では、専用のＩＣカードを用いて受信機と認証・課金機関（あるいはセンター）との間の電話回線を通して利用者の個人情報や利用の許可情報、利用状況の情報を管理している。つまり、受信機には利用者と認証・課金機関との間の通信を行うための通信手段としてモデム（変復調器）が内蔵されており、モデム接続によって電話回線を通して利用者から認証・課金機関に対して個人情報や利用状況の情報が通知され、また、認証・課金機関から利用者には情報利用の許可情報が通知される。

【0004】

【発明が解決しようとする課題】しかしながら、従来の認証・課金機関と利用者との間の通信手段に関して下記に示すような問題点がある。

【0005】（ａ）通信設備が大掛かりである

（ｂ）装置の設置場所が制限される

（ｃ）パッケージメディアの再生装置への適用が困難である

（ｄ）利用者によって個人の特定が困難である

（ｅ）通信費用の低減が困難である。

【0006】まず、上記（ａ）については、装置のコスト上昇を招いたり、接続工事が必要になる。例えば、上記したデジタル衛星放送受信機では装置内に内蔵モデムが必要であり、また、モデムを電話回線に接続するための工事が必要となる。

【0007】そして、（ｂ）については、例えば、家庭内で受信機の内蔵モデムを電話回線に接続することのできる場所が限られている場合において、受信機の設置場所と受信情報の利用場所とが離れていると機器の接続作業が面倒である。

【0008】（ｃ）については、光ディスク（例えば、コンパクトディスク（ＣＤ）やミニディスク（ＭＤ）等。）等のパッケージメディアの再生装置に対してその内蔵モデムの接続という新たな工事を利用者に要求することは許容され難い。

【0009】（ｄ）については、情報提供に対する課金を、電話番号に基づいて行う方法では、真の利用者である個人を特定することが困難である場合が多い（例えば、家族全員で一つの電話を共用している場合等。）。

【0010】（ｅ）については、利用者個人の特定という点に関して携帯電話やＰＨＳ（Personal Handy phone System）では個人での使用比率が高いので、これらを利用する方法が考えられるが、通信費用が高いので少額の課金には不向きである。

【0011】そこで、本発明は、情報の利用にあたって、簡易な認証・課金機関と利用者との間の通信手段を確保することを課題とする。

【0012】

【課題を解決するための手段】本発明は上記した課題を解決するために、情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報、利用対象とされる情報又は当該情報内容を特定するために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知することによって、認証・課金機関が利用主体及び客体を特定する方法と、認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報（暗号解読鍵等）を配布する方法とを提案するものである。

【0013】従って、本発明によれば、認証・課金機関と情報利用者とは、電話回線と無線呼び出しという簡易な通信方法によって結び付けることが可能となる。

【0014】

【発明の実施の形態】図１は、本発明に係る概要の説明図であり、情報利用者についての認証・課金方法及び当該利用者への情報復元用情報の配布方法について示すものである。

【0015】尚、ここでいう「情報」には、音声情報や映像情報等の情報や、コンピュータ機器で使用する情報等、一切の情報が含まれ、デジタル情報、アナログ情報の如何は問わない。また、本発明に關する限り情報利用者への情報の伝達形態が特定されることはなく、光ディスク等の情報記録媒体から再生される情報や、有線又は無線通信（コンピュータネットワークや衛星通信等。）を通して受信される情報等、各種の情報に利用することができる。

【0016】図１において、主体は情報利用者として、認証・課金機関である。

【0017】認証・課金機関は、情報利用者の加入登録情報に基づいて当該利用者に利用料金を請求する機関であり、認証・課金処理装置１を有する。

【0018】情報利用者から認証・課金機関への通信接続（アップリンク）には、電話回線が用いられ、情報利用者は、希望の情報を利用するために先立って、下記に示す情報を電話２で認証・課金機関に通知する。

【0019】（１）情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報

（１）利用対象とされる情報又は当該情報内容を特定するために予め付与されている識別情報。

【0020】先ず、（１）の情報は、情報利用者によってするために必要であり、個人情報には、氏名、住所、電話番号等の他、クレジットカード番号、利用金融機関や口座番号等が含まれる。

【0021】また、（１）の情報は、情報利用者が利用を意図している情報を特定するために必要な情報であり、例えば、情報記録媒体に付された識別番号、番組情報やプログラム番号、タイトルＩＤ等が挙げられる。

【0022】認証・課金機関はこれらの情報について、例えば、(音声)電話回線を介してトーン信号や無線呼び出しによる文字情報等と情報利用者から通知を受けることで、利用主体及び客体を特定する。

【0023】尚、個人情報の漏洩等に起因する損害の発生を防ぐためには、情報利用者の本人確認のためにパスワード(暗証番号や暗号コード等の暗号情報。)を要求することがセキュリティを高める上で望ましい。

【0024】即ち、情報利用者が上記した情報(Ⅰ)、(Ⅰ)に加えてパスワードを認証・課金機関に通知すると、該認証・課金機関は当該パスワードを、情報利用者について予め設定されているパスワードと照合することによって当該利用者の本人確認を行う。

【0025】認証・課金機関は、上記(Ⅰ)の情報から作成される加入登録情報に基づいて、上記(Ⅰ)の情報の利用に対する課金情報を集計した後、情報利用者への代金支払い請求・集金を行う。尚、図では、説明の便宜上、認証・課金機関を一の機関としているが、認証機関と課金・徴収機関とを分離しても良いことは勿論である。また、徴収した金額から、著作権者に使用料が還元されることは勿論である。

【0026】不正な情報の取得、複製等を防止するためには、利用対象である情報に暗号化処理を施したり、スクランブル処理(伝送情報の盗聴等を防止するために情報を復乱させる処理)等を実施することが効果的であり、そのためには、認証・課金機関が正式に認知した情報利用者に対してのみが正規の情報提供サービスを受けられるようにすることが好ましい。

【0027】つまり、情報利用者に対してその加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報(暗号解読用の鍵情報等であり、図には鍵の図形で示す。)を配布する。

【0028】例えば、情報利用者が無線呼び出し装置3としてのページャー機(所謂ポケットベル)を所持しており、認証・課金機関から該情報利用者への通信(ダウンリンク)において、ページャー機を呼び出して情報復元用情報(これを「KY」と記す。)を通知する。尚、その際、利用対象とされる情報の識別情報も併せて通知されることは勿論である。例えば、ページャー機は、文字や図形情報を表示するための表示手段4を有しているので、上記情報(Ⅰ)及び情報復元用情報を、認証・課金機関から受信した際に、これらの情報が文字情報として表示される。

【0029】正規に加入登録した情報利用者は、情報復元用情報(KY)を再生又は受信装置5に入力することによって、利用を意図する情報に施された暗号化等の秘匿処理を解除して、有意味な情報を取り出すことができる。つまり、情報の再生又は受信装置5内には、再生情報

又は受信情報の復号化等を行うための復元元処理部6が設けられており、該復元元処理部6は、情報復元用情報(KY)を用いて情報を復元(暗号化の解除等。)し、情報利用者による直接の利用が可能な形態に変換する。

【0030】尚、無線呼び出しによって情報利用者へ通知される情報復元用情報の漏洩や盗聴等を未然に防止するためには、情報復元用情報に対して暗号化を施しておき、この暗号化された情報復元用情報を再生又は受信装置5に入力したときに、当該情報に施された暗号化を、予め設定されている鍵情報を用いて解除するとともに、解除後の情報復元用情報に基づいて、利用対象である情報の復元元処理を行うことが望ましい。

【0031】つまり、この場合には、下記に示す(i)乃至(ii)の手順を採る。

【0032】(i)利用対象とされる情報毎に付与される情報復元用情報を、認証・課金機関と情報利用者との間で適用する鍵情報を用いて認証・課金機関が暗号化する

(ii)(i)で暗号化された情報復元用情報を、認証・課金機関が情報利用者への無線呼び出しによって当該利用者へ通知する

(iii)(ii)で通知された情報復元用情報に施された暗号化を、情報利用者が(i)の鍵情報と同じ鍵情報を用いて解除する。

【0033】例えば、図2に示すように、情報復元用情報を鍵情報「A」とする場合において、これを鍵情報「B」によって暗号化する(図には、鍵情報Aを箱詰めにした後、これに付する鍵前シに鍵情報Bで鍵をかいた状態の図で概念的に示す。)。

【0034】この作業は認証・課金機関によって行われ、秘匿化された鍵情報Aが情報利用者のページャー機に通知される。例えば、暗号化された鍵情報Aがページャー機に文字情報として表示される。

【0035】情報利用者は、事前に所有している鍵情報Bを使って鍵情報Aの暗号化を解除してこれを取り出す(図には、箱詰めにした鍵情報Aに付設された鍵前シに鍵情報Bを外した状態の図で概念的に示す。)。

【0036】そして、この鍵情報Aを使って利用対象である情報「H1」に施された暗号化を解除する(図には、箱詰めにした情報H1に付設された鍵前シを鍵情報Aで外した状態の図で概念的に示す。)。これによって、情報利用者は有意味な情報の利用が可能になる。このように、利用対象である情報及びその情報復元用情報の両者に対して秘匿処理を施すことによって2重の安全対策を講じることができる。

【0037】本発明に使用する無線呼び出し装置においては、図3に示すように、情報復元用情報(KY)を情報の再生又は受信装置5に伝送するための送信手段7を設けることが好ましい。即ち、情報復元用情報を再生又は受信装置5に伝送する方法には、再生又は受信装置に

操作入力部を付設して、キー操作入力によって手動で情報復元用情報を入力する方法があるが、無線呼び出し装置3に送信手段7を設けるとともに、再生又は受信装置5には、情報復元用情報を装置内に取り込むための受信手段8を設けることによってキー入力の手間を省くことができる。尚、図6では、無線呼び出し装置3内の受信部9で受信した情報復元用情報(KY)を表示手段4に送出して表示するとともに、送信手段7から再生又は受信装置5の受信手段8を介して復元化処理部6に情報復元用情報が送信される。

【0038】また、送信手段7から受信手段8への情報の伝送形態については有線方式又は無線方式(赤外線や微弱電波等の電磁波、音声、超音波等を用いる。)が挙げられるが、後者の方が便利である。この他、図4に示すように、無線呼び出し装置3を再生又は受信装置5に装着して情報を受け渡す方法の場合には、カードパス等のインターフェース部を用いた端子接続(無線呼び出し装置3に設けられた送信側の端子部7Aと、再生又は受信装置5に設けられた受信側の端子部8Aとを接続する。)によって情報を直接的に取り出せるので、無線呼び出し装置3をあたかもICカードのように取り扱うことができる。

【0039】

【実施例】図5及び図6は光学読取式の情報記録媒体(例えば、コンパクトディスクやミニディスク等の光ディスク)を用いたパッケージメディアの再生システムに本発明を適用した実施の一例を示すものである。尚、本発明に関する限り、情報記録媒体についての形態の如何は問わないので、ディスク状に限らず、テープ状、シート状、カード状等、各種の媒体に幅広く適用することができることは勿論である。

【0040】図5は認証、課金システムと光ディスクの再生装置を示すものであり、光ディスク10の記録情報については鍵情報「A」によって暗号化が施されている(図には、光ディスクそのものに付した錠前Mに鍵情報Aで鍵をかけた状態の図で概念的に示す。)。よって、該光ディスクの記録内容を取り出すのに通常の再生動作では不十分であり、暗号化の解除を必要とする。

【0041】この光ディスク10を入手したユーザー(情報利用者)は、先ず、認証・課金センターに電話をかける。

【0042】認証・課金センターでは、例えば、自動応答システムが導入された処理装置を用いて音声ガイドが行われ、ユーザーはガイド音声に従ってプッシュボタンを操作し、これによって発生するトーン信号によって、必要な情報を認証・課金センターに通知する。尚、ここで必要な情報とは、ポケットベル番号、暗証番号、光ディスク又はコンテンツ(情報内容)に固有の識別情報(1D番号)等である。

【0043】認証・課金センターは、先ず、通知された

ポケットベル番号及び暗証番号に基づいて相手が正規に登録済のユーザーであるか否かを判断する。そして、正規登録ユーザーの確認がとれた場合に、当該ユーザーに対して光ディスクやコンテンツに固有の識別情報を要求する。ユーザーは要求された識別情報を入力し、これを受けて認証・課金センターは、当該識別情報に対応した鍵情報(この場合は、鍵情報「B」を、別の鍵情報「B」(ユーザーと認証・課金センターとの間で予め定められている。))を使って暗号化(図5の錠前M参照。)した後、これをユーザーの所有するポケットベル11に送信する。尚、ポケットベルは小型軽量の個人携帯端末であるため、特に携帯用の再生装置への適用(再生装置と組みにした使用)が容易であり、また、サービスエリアが広いため基地局の設置や維持に必要な費用が少なくて済むといった利点がある。

【0044】認証・課金センターでは、その後、暗号化された鍵情報Aの送信が完了した時点で、ポケットベル番号に対応する加入登録情報に従って課金・取扱い処理を行う。つまり、暗号化された鍵情報Aの発行時点での課金が可能であり、これによって利用料金の徴収についての確実性を高めることができる。

【0045】このように暗号化された鍵情報Aはユーザーのポケットベル11で着信されるが、当該情報を再生装置12に入力又は転送する方法には、例えば、下記の(1)乃至(4)に示す方法が挙げられる。

【0046】(1)ポケットベルの表示部(液晶式ディスプレイ等)に文字表示される鍵情報を見て、ユーザーがキー操作で再生装置に入力する方法

(2)ポケットベルに設けられたカードインターフェースによって、ポケットベル本体を再生装置に装着して鍵情報を転送する方法

(3)ポケットベルに付設された通信用の発光部(発光ダイオード等)によって赤外線を発して、これを再生装置の受光部(フォトダイオード等)で受光することで鍵情報を転送する方法

(4)ポケットベルに付設された発信部によって微弱な電波を発信し、これを再生装置の受信部で受け取ることによって鍵情報を転送する方法。

【0047】こうして再生装置に伝送された鍵情報Aは、予め装置内に用意されている鍵情報Bを使って復号化される(錠前Mが外される。)。そして、この復号化された鍵情報Aによって、光ディスク10の記録情報に施された暗号化が解除(復号化)されて(錠前Mが外される。)、情報の再生が可能となる。

【0048】図6は以上の手順を時間の順序に従ってまとめたものであり、下記(1)乃至(5)に示す通りである。

【0049】(1)ポケットベル番号・暗証番号の通知
(2)コンテンツID(識別情報)の要求

(3)コンテンツIDの通知

(4) 鍵情報Aの送信

(5) 鍵情報Aの受信確認

尚、奇数番号で示す手続がユーザーから認証・課金センターに対して行われ、偶数番号で示す手続が認証・課金センターからユーザーに対して行われる。

【0050】図7は、本発明をデジタル衛星放送におけるユーザー認証・課金方法及びシステムに適用した実施の一例を示すものである。

【0051】放送業者と認証・課金センターとは専用回線で結ばれており、放送業者は放送衛星を介して、ユーザーの使用する受信装置13に情報を送信する。

【0052】ユーザーと認証・課金センターとの間の通信については、電話回線及び無線呼び出しによって上記した説明と同様に行う。即ち、上記の説明において、

「光ディスクの記録情報」を「受信を意図する情報（番組情報等）」とし、また、鍵情報Aによる情報の「略号化」を「略号化あるいはスクランブル処理」とする等の読み替えを適宜に行えば良い。要するに、この場合にはユーザーの認証及びコンテンツの識別情報の通知が電話回線を介して認証・課金センターに行われた後、該センターからユーザーに対してコンテンツの利用を許可するための情報（スクランブル処理の解除（デスクランブル）用情報等）又は当該情報を鍵情報Bで暗号化した情報がユーザー所有のポケットベル11に通知される。

【0053】デジタル衛星を利用した従来のシステムでは、受信装置にモデム等の通信手段を設けて当該受信装置と認証・課金センターの処理装置との間で電話回線で接続する必要があるが、本発明ではこのような通信手段を受信装置に設ける必要がないので、受信装置の設置場所が制限されることはない。

【0054】また、従来のシステムではユーザーの個人情報や許可情報、利用状況の情報等を格納する専用カード（ICカード）を受信装置に装着する必要があるが、上記のように、個人用携帯端末であるポケットベルを、ユーザー個人の認証・課金用のカードとして代用することによって認証・課金センターとの通信手段を容易に確保することができる。しかも、ポケットベルは、比較的な安値に利用することができ普及率も高いので少額課金のシステムへの利用にとって有利であり、利用料金の徴収時にも活用することができる。そして、ポケットベルは、他の携帯端末に比べて個人の使用比率が高く、また、契約しにくいと使用できない携帯端末であるため、個人の特定が容易である。

【0055】図8はインターネットを利用してコンピュータ機器に音楽情報を配布するシステムに本発明を適用した例を示すものである。

【0056】ユーザーは、まず、コンピュータ（PC）及びモデム等の通信手段を使ってインターネット経由で情報提供機関の会員データベースにアクセスし、自分のID（識別）番号及びパスワードを入力する。

【0057】ユーザーの認証が済むと、ユーザーはWWW（World Wide Web）ブラウザ（閲覧ソフト）を使って自分の意図する音楽ソフトの配信情報を情報提供機関に依頼する。

【0058】これを受けて情報提供機関は、配信サーバを用いて、コンテンツ・データベースに格納されている音楽ソフトの中からユーザーから依頼されたものを検索し取り出し、これに暗号化及び電子透かしを施した情報（図には、音符記号で示す音楽ソフトを箱詰めにした上でその鍵前Mに鍵情報「A」で鍵をかけた状態の図で概念的に示す。）をインターネット経由でユーザーのコンピュータ（PC）に送信することでダウンロードが完了する。尚、「電子透かし」とは音声情報の中に耳では聞えないように情報を重複して埋め込む方式（スペクトラム拡散等を利用する。）であり、本例ではコンテンツ（この場合は音楽情報）の識別情報に対して用いている。

【0059】ユーザーは、ダウンロードした情報をそのままでは利用することができないので、音楽ソフトに施された電子透かしからコンテンツの識別情報を再生してこれを知り、情報提供機関に電話をかけた後認証・課金に必要な情報及びコンテンツの識別情報を通知する。

【0060】情報提供機関からはユーザーのポケットベル11に、上記鍵情報Aを別の鍵情報「B」で暗号化した情報（図には、鍵情報Aを箱詰めにした上でその鍵前Mに鍵情報Bで鍵をかけた状態の図で概念的に示す。）が通知されるので、ユーザーは当該情報をコンピュータ（PC）に入力する。これによって事前に用意されている鍵情報Bを使って鍵情報Aの復号化を行う。

【0061】こうして、元の鍵情報Aが行われるので、これを使って音楽ソフトの復号化を行うことができる。

【0062】尚、鍵情報Aや音楽ソフトの復号化処理は、コンピュータ（PC）上でソフトウェア処理により実現される専用プレーヤ（音楽再生用ソフトウェア）で行われ、ここでは鍵情報Aで暗号化された音楽ソフトが鍵情報Aで暗号化されたファイルとして取り扱われ、ユーザーが鍵情報Bで暗号化された鍵情報Aを入力すると、鍵情報Aの復号化、これに続く音楽ソフトの復号化が行われて音楽ソフトの再生が可能となる。また、ユーザーが音楽ソフトを受け取る経路と、暗号化された鍵情報を受け取る経路とを分けることによって安全性を高めることができる。

【0063】しかし、本発明によれば、情報の配布形態の如何に関係なくユーザーの認証・コンテンツに係る課金システムに幅広く適用することができる。

【0064】また、同一のコンテンツであっても、該コンテンツのID（識別情報）毎に暗号鍵を変えることによってセキュリティ面の強化が可能であり、また、加入登録者又は使用する機器毎に鍵情報Bを変えたり、あるいはこれを時間の経過に伴って更新していく方法によ

り、さらに高いセキュリティを維持することができる。

【0065】

【発明の効果】以上に記載したところから明らかなように、請求項1に係る発明によれば、電話回線を通して必要な情報を認証・課金機関に通知することで、認証・課金機関が利用主体及び客体を特定することができるので、通信設備が大掛かりにならず、また、使用装置の設置場所が制限されない、また、パッケージメディアの再生装置への適用、利用者個人の特定等が容易である。

【0066】請求項2に係る発明によれば、情報利用者が電話回線を通して認証・課金機関にパスワードを送出して認証・課金機関により情報利用者の確認が行われるので、他人による不正な利用を防止することができる。

【0067】請求項3に係る発明によれば、認証・課金機関が、情報利用者への無線呼び出しによって当該利用者個人を特定して情報復元用情報を配布することができる、また通信費用の低減や通信設備の簡易化を図るとともに、装置の使用場所についての制約を排除することができる。

【0068】請求項4に係る発明によれば、情報復元用情報に対して暗号化を施すことによって当該情報の配布時の漏洩に起因する損害の発生を防止することができる。

【0069】請求項5、6に係る発明によれば、認証・課金機関から受信した識別情報や情報復元用情報を文字情報として表示することによって、これらの情報を情報利用者が直ちに認識して利用することができる。

【0070】請求項7乃至10に係る発明によれば、情報の再生又は受信を行う装置に対して、情報復元用情報を送信手段によって伝達することで、当該装置への情報の入力を容易に行うことができる。

【0071】請求項11に係る発明によれば、情報復元用情報の入力機能や情報の復元化機能を有する装置での

み有意な情報の利用が可能となるので、不正な情報利用の可能性を排除することができる。

【0072】請求項12に係る発明によれば、利用対象情報及び情報復元用情報に対して暗号化を施すことによって2重の安全対策を講じることができる。

【0073】請求項13、14に係る発明によれば、無線呼び出し装置から情報復元用情報を容易に取り込むことができる。

【図面の簡単な説明】

【図1】本発明に係る概要の説明図である。

【図2】情報復元用情報の暗号化・復号化と情報復元用情報による秘匿情報の復元についての説明図である。

【図3】無線呼び出し装置から再生又は受信装置への通信形態について説明するための概略図である。

【図4】無線呼び出し装置と再生又は受信装置との端子接続による通信形態について説明するための概略図である。

【図5】図6とともに、光学読取式の情報記録媒体を用いたパッケージメディアの再生システムに本発明を適用した実施の一例を示すものであり、本図は認証・課金システム及び光ディスクの再生装置についての説明図である。

【図6】処理手順を時間経過に沿って示す説明図である。

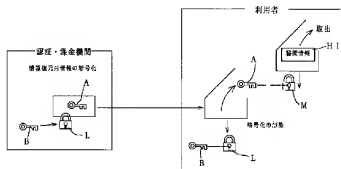
【図7】本発明をデジタル衛星放送におけるユーザー認証・課金方法及びシステムに適用した実施の一例を示す図である。

【図8】インターネットを利用してコンピュータ機器に音楽情報を配布するシステムに本発明を適用した実施の一例を示す図である。

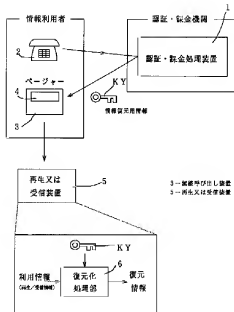
【符号の説明】

3…無線呼び出し装置、5…再生又は受信装置、7、7A…送信手段、8、8A…受信手段

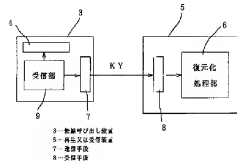
【図2】



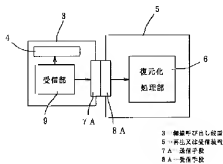
【図1】



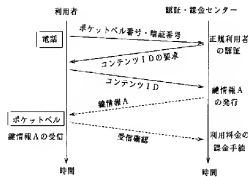
【図3】



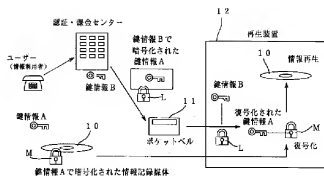
【図4】



【図6】



【図5】



【図7】

